Attorney Docket No. 122.1571

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Osamu ASANO

Application No.: Group Art Unit:

Filed: November 14, 2003 Examiner:

For: HUB UNIT FOR PREVENTING THE SPREAD OF VIRUSES, METHOD AND PROGRAM THEREFOR

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-335409

Filed: November 19, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: November 14, 2003 By: _____

H. J.Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月１９日

出願番号
Application Number: 特願２００２－３３５４０９

[ST. 10/C]: [ＪＰ２００２－３３５４０９]

出願人
Applicant(s): 富士通株式会社

２００３年 ７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０５７７６４

【書類名】　特許願
【整理番号】　0252360
【提出日】　平成14年11月19日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F　9/06
G06F 13/00
H01L 27/00
H04L 29/00
【発明の名称】　ウィルス拡散を防止する集線装置およびそのためのプログラム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　浅野　修
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100077517
【弁理士】
【氏名又は名称】　石田　敬
【電話番号】　03-5470-1900
【選任した代理人】
【識別番号】　100092624
【弁理士】
【氏名又は名称】　鶴田　準一

【選任した代理人】
　【識別番号】　100100871
　【弁理士】
　【氏名又は名称】　土屋　繁
【選任した代理人】
　【識別番号】　100082898
　【弁理士】
　【氏名又は名称】　西山　雅也
【選任した代理人】
　【識別番号】　100081330
　【弁理士】
　【氏名又は名称】　樋口　外治
【手数料の表示】
　【予納台帳番号】　036135
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9905449
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ウィルス拡散を防止する集線装置およびそのためのプログラム

【特許請求の範囲】

【請求項１】　複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

ウィルス検出情報を格納する第１記憶部と、

前記通信装置から受信したデータを一時蓄積する第２記憶部と、

前記第１記憶部に格納されたウィルスの検出情報に基づき、前記第２記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部と、

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、

を備えたことを特徴とするウィルス拡散を防止する集線装置。

【請求項２】　前記集線装置に接続された複数の通信装置の送信アドレスを格納する第３記憶部を備え、

前記拡散防止部は、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納する、

請求項１に記載のウィルス拡散を防止する集線装置。

【請求項３】　前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする、

請求項１または２に記載のウィルス拡散を防止する集線装置。

【請求項４】　複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

コンピュータを、

ウィルスの検出情報を格納する第１記憶部、

前記通信装置から受信したデータを一時蓄積する第２記憶部、

前記第１記憶部に格納されたウィルスの検出情報に基づき、前記第２記憶部に

一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部、および

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部、

として機能させる、

ことを特徴としたウィルス拡散を防止する集線装置のためのプログラム。

【請求項５】　コンピュータを、

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第３記憶部として機能させ、かつ

前記拡散防止部が、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納するよう機能する、

請求項４に記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信ネットワークにおけるウィルス拡散を防止する集線装置（ＨＵＢユニット）およびそのためのプログラムに関する。

【０００２】

【従来の技術】

近年、通信技術の発展に伴いインターネット等の通信ネットワークを介したコンピュータ間および／または携帯電話間でのデータ通信が頻繁に行われるようになってきた。このようなネットワークに接続されたコンピュータに侵入し悪意に内部のデータを破壊したり外部に持ち出したりするウィルスが知られている。特に、企業内のコンピュータには機密情報が格納されているため企業にとってはウィルス対策が重要な課題になっている。このため、企業では、インターネットやイントラネットに接続された社内ホストコンピュータを外部から侵入するウィルスの感染から守るための装置（ファイアウォール）を導入している。

【０００３】

従来技術によるウィルス感染防止対策には、以下に記すようなウィルスチェックネットワークがある（下記の特許文献１参照）。

【０００４】

このウィルスネットワークは、ネットワークに接続された個々のコンピュータにウィルス感染防止用のワクチン・ソフトウェアを導入する場合、新種のウィルスが発見される度に個々のコンピュータでその新種のウィルス対策を施したワクチン・ソフトウェアに更新しなければならず、これを各コンピュータのユーザに徹底させるのは困難であり非効率的であることから、これを効率的に行うことを目的としたものであり、ウィルスパターン格納手段と、ウィルスパターンに基づき受信したパケットがウィルス感染しているか否かをネットワーク側でチェックするウィルスチェック手段と、ウィルス感染が検出されたパケットに感染ビットを付加して該パケットを送信するパケット送信手段とを備えるウィルスチェック装置と、前記ビットに基づいて感染パケットを検出する感染パケット検出手段と、該感染パケットに対応するファイルを実行不可にするファイル実行制御手段とを備えるクライアント端末と、ウィルスパターン情報をマルチキャストで前記ウィルスチェック装置に配布するウィルスパターン情報配布手段と、前記ウィルスパターン情報を一元管理するウィルス情報管理手段とを備えるウィルス情報管理局と、を具備して構成される。

【０００５】

また、他の従来技術によるウィルス感染防止対策には、コンピュータ回線網に接続されている受信側装置がコンピュータウィルスに感染した通信データを受信しないようにして受信側装置のコンピュータウィルスによる感染を未然に防ぐことを目的とし、コンピュータ回線網からデータを受信する受信処理手段と、受信データがウィルス感染しているかどうかを診断する受信データ処理手段と、受信データがコンピュータウィルスに感染している場合、これを示す感染信号を受信側装置に知らせる受信側装置間通信処理手段と、受信データがコンピュータウィルスに感染していない場合、受信データを受信側装置に送信する送信処理手段とを備えて構成したコンピュータウィルス受信監視装置およびコンピュータウィルス受信監視装置より感染信号を受信したときには受信データを受信しない受信側

装置がある（下記の特許文献２参照）。

【０００６】

【特許文献１】

特開平１１－１６７４８７号公報（明細書の［特許請求の範囲］の特に［請求項１］と［請求項１０］、［発明の詳細な説明］における段落番号［０００５］～［００１２］および図面の図１参照）

【特許文献２】

特開平１０－３０７７７６号公報（明細書の［特許請求の範囲］の特に［請求項１］と［請求項３］、［発明の詳細な説明］における段落番号［０００４］～［００１４］および図面の図１参照）

【０００７】

【発明が解決しようとする課題】

しかしながら、上記特許文献１に開示のウィルスチェックネットワークは、ウィルス感染防止のために、少なくとも伝送されるパケット（データ）にウィルス感染有無を示すビットを付すウィルスチェック装置、とそのビットに応じてウィルス侵入防止するクライアント端末と、が必須であり、全てのクライアント端末にウィルス侵入防止対策を施す必要がある。

【０００８】

一方、上記特許文献２に開示のコンピュータウィルス受信監視装置もまた、コンピュータウィルス受信監視装置と受信側装置とが必須であり、全ての受信側装置に感染信号を受信したときには受信データを受信しない構成を設けなければならない。

【０００９】

つまり、従来技術によれば、データを受信する全てのコンピュータに感染したデータを除去する構成を設ける必要があり、これを徹底するのは困難であるという問題を有する。

【００１０】

それゆえ、本発明は、上記問題を解決し、すなわちデータを受信する全てのコンピュータにウィルス侵入防止対策を施さなくてもウィルス侵入を防止しかつウ

ィルスの二次感染を防止することのできるウィルス拡散防止機能を備えた集線装置およびそのためのプログラムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成する本発明のウィルス拡散防止機能を備えた集線装置は、複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、ウィルスの検出情報を格納する第１記憶部と、通信装置から受信したデータを一時蓄積する第２記憶部と、前記第１記憶部に格納されたウィルスの検出情報に基づき、前記第２記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部と、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、を備えたことを特徴とする。

【００１２】

上記本発明のウィルス拡散防止機能を備えた集線装置において、前記集線装置に接続された複数の通信装置の送信アドレスを格納する第３記憶部を備え、前記拡散防止部は、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納する。

【００１３】

上記本発明のウィルス拡散防止機能を備えた集線装置において、前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする。

【００１４】

【発明の実施の形態】

以下、添付図面を参照しつつ本発明の実施の形態を詳細に説明する。

【００１５】

図１は本発明の第一実施形態に係るウィルス拡散防止機能を備えた集線装置の概略構成図である。図１に示す集線装置１は、ＩＥＥＥ８０２．３規格で規定す

る１０ＢＡＳＥ－Ｔに準拠したハブ（Ｈｕｂ）と称するものであり、一般的にスター形の物理的トポロジーによりネットワーク装置を接続できる物理的なポートが８ポートや１６ポート等、多数用意されている。ここで、ネットワーク装置とは、ＰＣ、ワークステーション、ゲートウェイ、ルータ等のコンピュータや他の集線装置を言う。

【００１６】

集線装置１は、１６ポートを有するものであり、ポートＰ１に接続されたコンピュータＰＣ１から受信したデータをＰＣ１のポートＰ１を除く他の全てのポートＰ２～Ｐ１６に（リピータハブ）、またはデータの宛先であるＰＣが接続されているポートのみに（スイッチングハブ）送信するための中継機能を有する。しかしながら、これらのポートＰ１～Ｐ１６は必ずしも全て使用されない場合が多い。図１は１６ポートを有する集線装置１に、４ポートしかネットワーク装置（例えば、ＰＣ１～ＰＣ４）が接続されていない例を示している。また、ポート３とポート４に接続されているネットワーク装置（例えばＰＣ３、ＰＣ４）の電源が切れている等、集線装置１にケーブルが接続されていても、集線装置１に接続されたネットワーク装置がアクティブでない場合がある。このような場合でも、前者の集線装置１は、例えばポートＰ１から受信したデータをポートＰ１以外のポート、すなわちポートＰ２からポートＰ１６に出力する機能を有する。

【００１７】

集線装置１は、ポートＰ１～Ｐ１６に接続された半導体装置（ＬＳＩ）２を有し、ＬＳＩ２は、ポートＰ１～Ｐ１６が接続されるポート部２１、リピータコントローラ２２およびウィルス処理部２３を有する。ポート部２１およびリピータコントローラ２２については図２～４を用いて後述する。

【００１８】

ウィルス処理部２３は、ウィルスのパターン情報を格納する第１記憶部２１１と、所定のネットワーク装置（コンピュータ）から受信したパケットを一時蓄積する第２記憶部２１２と、第１記憶部２１１に格納されたウィルスのパターンと第２記憶部２１２に一時蓄積されたパケットとを比較しパケットがウィルスに感染しているか否かを判定するウィルス検出部２１３と、ウィルス検出部２１３で

パケットがウィルスに感染していると判定されたとき、パケットを集線装置１に接続された前記所定のネットワーク装置（コンピュータ）以外のネットワーク装置（コンピュータ）に送信しないようにする拡散防止部２１４と、各ポートに接続されたネットワーク装置（コンピュータ）の送信アドレス（ＭＡＣアドレス）を格納する第３記憶部２１５とを有する。ここで、ＭＡＣアドレスとは、イーサネット（登録商標）などのＬＡＮで利用する通信回線に必要とされるもので、物理的な回線に接続されているコンピュータにセットされたＬＡＮボードなどを識別するためのアドレスのことである。

【００１９】

拡散防止部２１４は、ウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、そのパケットに付されたパケットの送信先コンピュータのアドレスが第３記憶部２１５に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、その送信アドレスに対応するコンピュータにパケットを送信しないようにするように構成してもよい。

【００２０】

ウィルス処理部２３は、一般的なディジタルコンピュータからなり、図示しない双方向性バスを介して相互に接続されたＣＰＵ、ＲＡＭ、ＲＯＭ、入力ポートおよび出力ポート等を具備する。

【００２１】

図２～４は本発明の第１～３実施例の集線装置を示す図であり、図５はリンクパルスと送受信データを示すタイムチャートである。図２～４に示す第１～３実施例の集線装置１は、半導体装置（ＬＳＩ）２、抵抗、送信トランス、受信トランスおよびコネクタを有する。コネクタは図１に示すポートに相当し、図１に示すように、集線装置１に例えばＰＣ１～ＰＣ４のパーソナルコンピュータを接続するためのものである。ＬＳＩ２は、ｎ個、本実施例では１６個の「ポートｎ」と示す第ｎポート部２１ｎと１つのリピータコントローラ２２とウィルス処理部２３とを有する。第ｎポート部２１ｎは、送信ブロック５０と受信ブロック６０とを有する。上記抵抗、送信トランス、受信トランスおよびコネクタは、第ｎポート部２１ｎ毎にそれぞれ設けられている。

【００２２】

送信ブロック５０は、リンクパルス生成回路５１、送信データ生成回路５２、ドライバ回路５３および節電回路５４を有する。リンクパルス生成回路５１は、リピータコントローラ２２から送信される、本実施例では１０ＭＨｚの送信ブロックシステムクロック（以下、単に送信クロックと記す）から図５の上段に示すようなリンクパルスを生成する。ここで、リンクパルスとは、ＩＥＥＥ８０２．３規格で定義されたものであり、図５に示すように、１０ｍｓ毎に１００ｎｓのパルスを出力するものである。

【００２３】

送信データ生成回路５２は、リピータコントローラ２２から送信される、送信クロック、図５の中段および下段に示すような最小６４バイトから最大１５００バイトの送信データおよび送信データが有効のときＨｉｇｈレベルとなる送信データイネーブル信号を受け、集線装置１から外部に送信する送信データを生成する。ここで、送信データは、１ビット当たり１００ｎｓのビットレートで送信されるので、最小送信データで約０．０５（ｍｓ）（＝６４×８×１００（ｎｓ））、最大送信データで約１．２（ｍｓ）（＝１５００×８×１００（ｎｓ））の送信時間を要する。ドライバ回路５３は、上記送信信号を増幅して出力する。

【００２４】

節電回路５４は、ドライバ回路５３の出力を停止する回路であり、送信ブロック５０の消費電力を削減するために設けた回路である。受信ブロック６０内のリンクパルス検出回路６１により検出されたリンク情報を元に、節電回路５４をなすＡＮＤゲート、ＡＮＤ１、ＡＮＤ２、ＡＮＤ３およびＡＮＤ４は制御される。リンク検出の結果がインアクティブ（この場合Ｌｏｗ）である場合、節電回路５４のＡＮＤゲートの出力はすべてＬｏｗレベルになる。この結果、リンク検出の結果がインアクティブであるポート、すなわちネットワークがアクティブでないポートの送信ブロック５０の出力電流を削減することが可能になり、消費電力が削減される。次に、受信ブロック６０について説明する。

【００２５】

受信ブロック６０は、リンクパルス検出回路６１、ＰＬＬ６２、受信データ再

生回路６３および送信阻止部６４（図２）、６５(図３)、６６(図４)を有する。リンクパルス検出回路６１は、ポートを介して受信トランスから受信されるリンク情報を元に、節電回路５４をなすＡＮＤゲート、ＡＮＤ１、ＡＮＤ２、ＡＮＤ３およびＡＮＤ４を制御する。リンク検出の結果がインアクティブ（この場合Ｌｏｗ）である場合、節電回路５４のＡＮＤゲートの出力はすべてＬｏｗレベルになる。ＰＬＬ（Phase Lock Loop ）６２は、ポートを介して受信トランスから受信された受信データから受信クロックを生成する。

【００２６】

受信データ再生回路６３は、リンクパルス検出回路６１から受信データをＰＬＬ６２から受信クロックを受け、受信データを再生するとともに受信データが有効のときＨｉｇｈレベルとなる受信データイネーブル信号を生成する。送信阻止部６４～６６は、ウィルス処理部２３におけるウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、集線装置１に接続された前記所定のネットワーク装置（コンピュータ）以外のネットワーク装置（コンピュータ）に送信しないようにする拡散防止部２１４の出力ポートに接続される。この出力ポートは、ウィルス感染検出前にＨｉｇｈレベルとなり、ウィルス感染検出後にＬｏｗレベルとなる受信データディスエーブル信号を送信阻止部６４～６６に送る。

【００２７】

第２または第３実施例の拡散防止部２１４は、送信阻止部（第２または第３実施例）６５または６６により、ウィルス検出部２１３がウィルスに感染していると判定したパケットを検出した後、前記所定のコンピュータから新たにパケットを受信しないようにする。あるいは受信しても、他のコンピュータへ送信しないようにする。

【００２８】

第３実施例の拡散防止部２１４は、送信阻止部（第３実施例）６６により、ウィルス検出部２１３がウィルスに感染していると判定したパケットを検出した後、前記所定のコンピュータから新たに受信するパケットを無効にする。

【００２９】

第１～３実施例の集線装置１は、ウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、ウィルス感染したパケットが検出されたことを示す表示手段（図示せず）を備える。この表示によりコンピュータのユーザはウィルス感染の発生を知ることができる。

【００３０】

リピータコントローラ２２は、第ｎポート部２１ｎの何れか１つが受信した受信データ、受信データイネーブルおよび受信クロックを受け、（ｎ－１）個の他の第ｎポート部２１ｎへ送信ブロックシステムクロック、送信データおよび送信データイネーブルを送信する。

【００３１】

また、第ｎポート部２１ｎが送信中に受信すると、送信と受信が同時となるコリージョンという状態になる。この場合、リピータコントローラ２２は、次のようなコリージョン処理を実行する。全ポートにジャム信号と称する特定データを所定期間送信する。また、このコリージョンの原因となったＰＣ側、例えばＰＣ１、ＰＣ２も、内蔵するネットワークインターフェースカードによりジャム信号を所定期間送信する。ジャム信号が送信された後、集線装置１側およびＰＣ側は全て送信を中止し、次いでランダム時間待った後、コリージョンの原因となったＰＣ１、ＰＣ２は互いに時間間隔をもって送信を再開する。

【００３２】

次に、受信ブロック６０内の送信阻止部６４～６６について以下に詳述する。

【００３３】

図２に示す第１実施例の送信阻止部６４は、ＡＮＤゲートからなり、ＡＮＤゲートの一方の入力部には受信ブロック６０内のリンクパルス検出回路６１から送信ブロック５０内の節電回路５４への制御信号が、他方の入力部にはウィルス処理部２３からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部２１４の出力ポートから出力され、集線装置１内のウィルス処理部２３におけるウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、Ｈｉｇｈレベルから Ｌｏｗレベルに変化し、集線装置１に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウィ

ルス感染したパケットを送信したネットワーク装置（コンピュータ）以外のネットワーク装置（コンピュータ）にそのパケットを送信させない。

【００３４】

図３に示す第２実施例の送信阻止部６５は、２つのＡＮＤゲートからなり、各ＡＮＤゲートの一方の入力部には受信ブロック６０内のリンクパルス検出回路６１への受信信号が、他方の入力部にはウィルス処理部２３からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部２１４の出力ポートから出力され、集線装置１内のウィルス処理部２３におけるウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、ＨｉｇｈレベルからＬｏｗレベルに変化し、集線装置１に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウィルス感染したパケットを送信したネットワーク装置（コンピュータ）から新たなパケットを受信しないようにする。

【００３５】

図４に示す第３実施例の送信阻止部６６は、ＡＮＤゲートからなり、ＡＮＤゲートの一方の入力部には受信ブロック６０内の受信データ再生回路６３からリピータコントローラ２２への受信データイネーブル信号が、他方の入力部にはウィルス処理部２３からの受信データディスエーブル信号が入力される。受信データディスエーブル信号は、拡散防止部２１４の出力ポートから出力され、集線装置１内のウィルス処理部２３におけるウィルス検出部２１３でパケットがウィルスに感染していると判定されたとき、ＨｉｇｈレベルからＬｏｗレベルに変化し、集線装置１に接続された前記所定のネットワーク装置（コンピュータ）、すなわちウィルス感染したパケットを送信したネットワーク装置（コンピュータ）から新たに受信するパケットを無効にする。

【００３６】

次に、集線装置１の正常状態への復帰方法について説明する。上述したように、集線装置１は、パケットがウィルス感染していることを検出すると、二次感染防止するため、受信データディスエーブル信号をＨｉｇｈレベルからＬｏｗレベルにしてパケットを集線装置１の外部に送信しないようにする。このような状態

になったときは集線装置１の筐体に取付けた表示器（図示せず）を表示してユーザに知らせ、ユーザは例えば集線装置１の筐体に取付けたリセットボタン（図示せず）を押すことによりこれを解除して正常状態にする。集線装置１のウィルス処理部２３の拡散防止部２１４にこの復帰機能は設けられている。

【００３７】

図６は本発明の第二実施形態に係るウィルス拡散防止システムのブロック構成図である。図６全体に示すウィルス拡散防止システム１００は、パケット（データ）通信管理部１１０と集線装置部１２０とを備える。パケット通信管理部１１０はＷＡＮ／ＬＡＮを経由した後さらにＬＡＮを経由して集線装置部１２０に接続される。パケット通信管理部１１０は、具体的にはゲートウェイまたはルータを備える。パケット通信管理部（ゲートウェイまたはルータ）１１０には、ウィルスのパターン情報を格納する第１記憶部１１１ａと、所定のコンピュータから受信したパケットを一時蓄積する第２記憶部１１１ｂと、第１記憶部１１１ａに格納されたウィルスのパターンと第２記憶部１１１ｂに一時蓄積されたパケットとを比較しパケットがウィルスに感染しているか否かを判定するウィルス検出部１１１ｃとを備えたウィルス監視部１１１が設けられている。

【００３８】

ここで、ゲートウェイおよびルータは、物理層（第１層）、データリンク層（第２層）、ネットワーク層（第３層）、トランスポート層（第４層）、セション層（第５層）、プレゼンテーション層（第６層）およびアプリケーション層（第７層）の７階層からなる、コンピュータの異機種間通信を可能とするためのネットワークアーキテクチャとしてのＯＳＩ（Open Systems Interconnection；開放型システム間相互接続）の基本参照モデルにおいて、ゲートウェイはアプリケーション層の機能を果たし、ルータはネットワーク層の機能を果たす機器である。

【００３９】

集線装置部１２０は図１～４を用いて説明したものと同様な少なくとも１つの集線装置１２１からなる。集線装置１２１は、集線装置１２１に接続されたコンピュータの送信アドレスを格納する第３記憶部１２２ａと、パケット通信管理部１１０のウィルス検出部１１１ｃでパケットがウィルスに感染していると判定さ

れたとき、そのパケットの受信先コンピュータのアドレス情報をパケット通信管理部１１０から受け、そのパケットを集線装置１２１に接続されたそのパケットの受信先コンピュータ以外のコンピュータに送信しないようにする拡散防止部１２２ｂとを備えたウィルス処理部１２２を備える。

【００４０】

拡散防止部１２２ｂは、パケット通信管理部１１０内のウィルス検出部１１１ｃでパケットがウィルスに感染していると判定されたとき、そのパケットの送信先コンピュータのアドレス情報をパケット通信管理部１１０から受け、そのパケットに付されたパケットの送信先コンピュータのアドレスが第３記憶部１２２ａに格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、その送信アドレスに対応するコンピュータにパケットを送信しないようにする。

【００４１】

集線装置部１２０は、複数個の集線装置１２１がカスケード接続されており、拡散防止部１２２ｂは、パケット通信管理部１１０内のウィルス検出部１１１ｃでパケットがウィルスに感染していると判定されたとき、そのパケットの送信先コンピュータのアドレス情報をパケット通信管理部１１０２ら受け、そのパケットに付されたパケットの送信先コンピュータのアドレスが第３記憶部１２２ａに格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されなかったとき、カスケード接続された集線装置１２１で逐次上記同様の一致判定を行い、その結果が一致と判定されたとき、送信アドレスに対応するコンピュータにパケットを送信しないようにする。

【００４２】

図７は本発明の第１実施例のウィルス拡散防止システムを示す図である。パケット通信管理部１１０がゲートウェイ１１１であり、集線装置部１２０が２つの集線装置１２１－１と１２２－２を有する例を示す。集線装置１２１－１にはネットワーク装置である集線装置１ＰＣ１、（ｎ－１）個のコンピュータ１ＰＣ２、…、１ＰＣｎが接続されており、この内１個がルータ１１２である。集線装置１２１－１のウィルス処理部内の第３記憶部には各コンピュータ１ＰＣ２、…、

１ＰＣｎのＭＡＣアドレスが格納されている。集線装置１２１－２にはネットワーク装置であるｍ個のコンピュータ２ＰＣ１、２ＰＣ２、…、２ＰＣｋ、…、２ＰＣｍが接続されている。集線装置１２１－２のウィルス処理部内の第３記憶部には各コンピュータ２ＰＣ１、２ＰＣ２、…、２ＰＣｋ、…、２ＰＣｍのＭＡＣアドレスが格納されている。ここで、ｋ、ｎ、ｍは、正の整数であり、ｋ＜ｎ、ｋ＜ｍである。例えば、コンピュータ２ＰＣｋがウィルス感染したパケットの送信先であれば、第１実施例の集線装置では、集線装置１２２－２内のポートＰｋに接続された第ｋポート部２１ｋからの送信データがディスエーブルされ、ウィルス感染したパケットは集線装置１２２－１および１２２－２の外部に出力されない。一方第２、３実施例の集線装置では、対応する集線装置１２２－２内のポートＰｋに接続された第ｋポート部２１ｋへの受信データがディスエーブルされ、ウィルス感染したパケットは集線装置１２２－１および１２２－２の外部に出力されない。

【００４３】

図７に示す第１実施例のウィルス拡散防止システムでは、パケット通信管理部１１０がゲートウェイ１１１の例として説明したが、パケット通信管理部１１０はルータ１１２であってもよい。

【００４４】

（付記１）

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

ウィルスの検出情報を格納する第１記憶部と、

前記通信装置から受信したデータを一時蓄積する第２記憶部と、

前記第１記憶部に格納されたウィルス検出情報に基づき、前記第２記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部と、

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部と、

を備えたことを特徴とする。

【００４５】

（付記２）

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第３記憶部を備え、

前記拡散防止部は、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納する、

付記１に記載のウィルス拡散を防止する集線装置。

【００４６】

（付記３）

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置からの新たなデータを他の通信装置に送信しないようにする、

付記１または２に記載のウィルス拡散を防止する集線装置。

【００４７】

（付記４）

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置から新たにデータを受信しないようにする、

付記１乃至３の何れか一つに記載のウィルス拡散を防止する集線装置。

【００４８】

（付記５）

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置から新たに受信するデータを無効にする、

付記１乃至４の何れか一つに記載のウィルス拡散を防止する集線装置。

【００４９】

（付記６）

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、ウィルス感染したデータが検出されたことを示す表示手段を備える、

付記１乃至５の何れか一つに記載のウィルス拡散を防止する集線装置。

【００５０】

（付記７）

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置と該集線装置にネットワークを介して接続され前記通信装置間でデータを送受信するデータ通信管理部とを備えたウィルス拡散防止システムにおいて、

前記データ通信管理部は、ウィルスのパターン情報を格納する第１記憶部と、前記通信装置から受信したデータを一時蓄積する第２記憶部と、前記第１記憶部に格納されたウィルスのパターン情報と前記第２記憶部に一時蓄積された前記データとを比較し該データがウィルスに感染しているか否かを判定するウィルス検出部とを備え、

前記集線装置は、該集線装置に接続された通信装置の送信アドレスを格納する第３記憶部と、前記データ通信管理部の前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データの受信先通信装置のアドレス情報を前記データ通信管理部から受け、該データを前記集線装置に接続された前記受信先通信装置以外の通信装置に送信しないようにする拡散防止部とを備え、

たことを特徴とするウィルス拡散防止システム。

【００５１】

（付記８）

前記拡散防止部は、前記データ通信管理部内の前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データの送信先通信装置のアドレス情報を前記データ通信管理部から受け、該データに付された該データの送信先通信装置のアドレスが前記第３記憶部に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されたとき、該送信アドレスに対応する通信装置にデータを送信しないようにする、

付記７に記載のウィルス拡散防止システム。

【００５２】

（付記９）

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置から新たにパケットを受信しないようにする

、
付記７または８に記載のウィルス拡散防止システム。

【００５３】

（付記１０）

前記拡散防止部は、前記ウィルス検出部がウィルスに感染していると判定したデータを検出した後、前記通信装置から新たに受信するデータを無効にする、
付記７または８に記載のウィルス拡散防止システム。

【００５４】

（付記１１）

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、ウィルス感染したデータが検出されたことを示す表示手段を備えた、
付記７乃至１０の何れか一つに記載のウィルス拡散防止システム。

【００５５】

（付記１２）

前記集線装置は、複数個がカスケード接続されており、

前記拡散防止部は、前記データ通信管理部内の前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データの送信先通信装置のアドレス情報を前記データ通信管理部から受け、該データに付された該データの送信先通信装置のアドレスが前記第３記憶部に格納されている送信アドレスに一致するか否かを判定し、その結果が一致と判定されなかったとき、前記カスケード接続された前記集線装置で逐次上記同様の一致判定を行い、その結果が一致と判定されたとき、該送信アドレスに対応する通信装置にデータを送信しないようにする、
付記７乃至１１の何れか一つに記載のウィルス拡散防止システム。

【００５６】

（付記１３）

前記データ通信管理部は、ゲートウェイまたはルータである、
付記７乃至１２の何れか一つに記載のウィルス拡散防止システム。

【００５７】

（付記１４）

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

コンピュータを、

ウィルスの検出情報を格納する第１記憶部、

前記通信装置から受信したデータを一時蓄積する第２記憶部、

前記第１記憶部に格納されたウィルスの検出情報に基づき、前記第２記憶部に一時蓄積された前記データがウィルスに感染しているか否かを判定するウィルス検出部、および

前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信しないようにする拡散防止部、

として機能させる、

ことを特徴としたウィルス拡散を防止する集線装置のためのプログラム。

【００５８】

（付記１５）

コンピュータを、

前記集線装置に接続された複数の通信装置の送信アドレスを格納する第３記憶部として機能させ、かつ

前記拡散防止部が、前記ウィルス検出部で前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納するよう機能する、

付記１４に記載のプログラム。

【００５９】

（付記１６）

複数の通信装置を接続し該通信装置間でデータを送受信する集線装置において、

ウィルスの検出情報を第１記憶部に格納し、

前記通信装置から受信したデータを第２記憶部に一時蓄積し、

前記第１記憶部に格納されたウィルスの検出情報に基づき、前記第２記憶部に

一時蓄積された前記データがウィルスに感染しているか否かを判定し、

前記データがウィルスに感染していると判定されたとき、該データを前記集線装置に接続された前記所定の通信装置以外の通信装置に送信しないようにする、ことを特徴としたウィルス拡散を防止する集線装置のための方法。

【００６０】

（付記１７）

前記集線装置に接続された複数の通信装置の送信アドレスを第３記憶部に格納し、

前記データがウィルスに感染していると判定されたとき、該データを送信した通信装置のアドレスを前記第３記憶部に格納する、

付記１６に記載の方法。

【００６１】

【発明の効果】

以上説明したように本発明によれば、データを受信する全てのコンピュータにウィルス侵入防止対策を施さなくてもウィルス侵入を防止しかつウィルスの二次感染を防止することのできるウィルス拡散防止機能を備えた集線装置およびそのためのプログラムを提供することができる。

【図面の簡単な説明】

【図１】

本発明の第一実施形態に係るウィルス拡散防止機能を備えた集線装置の概略構成図である。

【図２】

本発明の第１実施例の集線装置を示す図である。

【図３】

本発明の第２実施例の集線装置を示す図である。

【図４】

本発明の第３実施例の集線装置を示す図である。

【図５】

リンクパルスと送受信データを示すタイムチャートである。

【図６】

本発明の第二実施形態に係るウィルス拡散防止システムのブロック構成図である。

【図７】

本発明の第１実施例のウィルス拡散防止システムを示す図である。

【符号の説明】

１、１２１－１、１２１－２…集線装置

２…半導体装置（ＬＳＩ）

２１…ポート部

２１ｎ…第ｎポート部

２２…リピータコントローラ

２３、１２２…ウィルス処理部

５０…送信ブロック

５１…リンクパルス生成回路

５２…送信データ生成回路

５３…ドライバ回路

５４…節電回路

６０…受信ブロック

６１…リンクパルス検出回路

６２…ＰＬＬ

６３…送信データ生成回路

６４、６５、６６…送信阻止部

１１０…パケット（データ）通信管理部

１１１…ウィルス監視部

１１１ａ、２１１…第１記憶部

１１１ｂ、２１２…第２記憶部

１２０…集線装置部

１２２ａ、２１５…第３記憶部

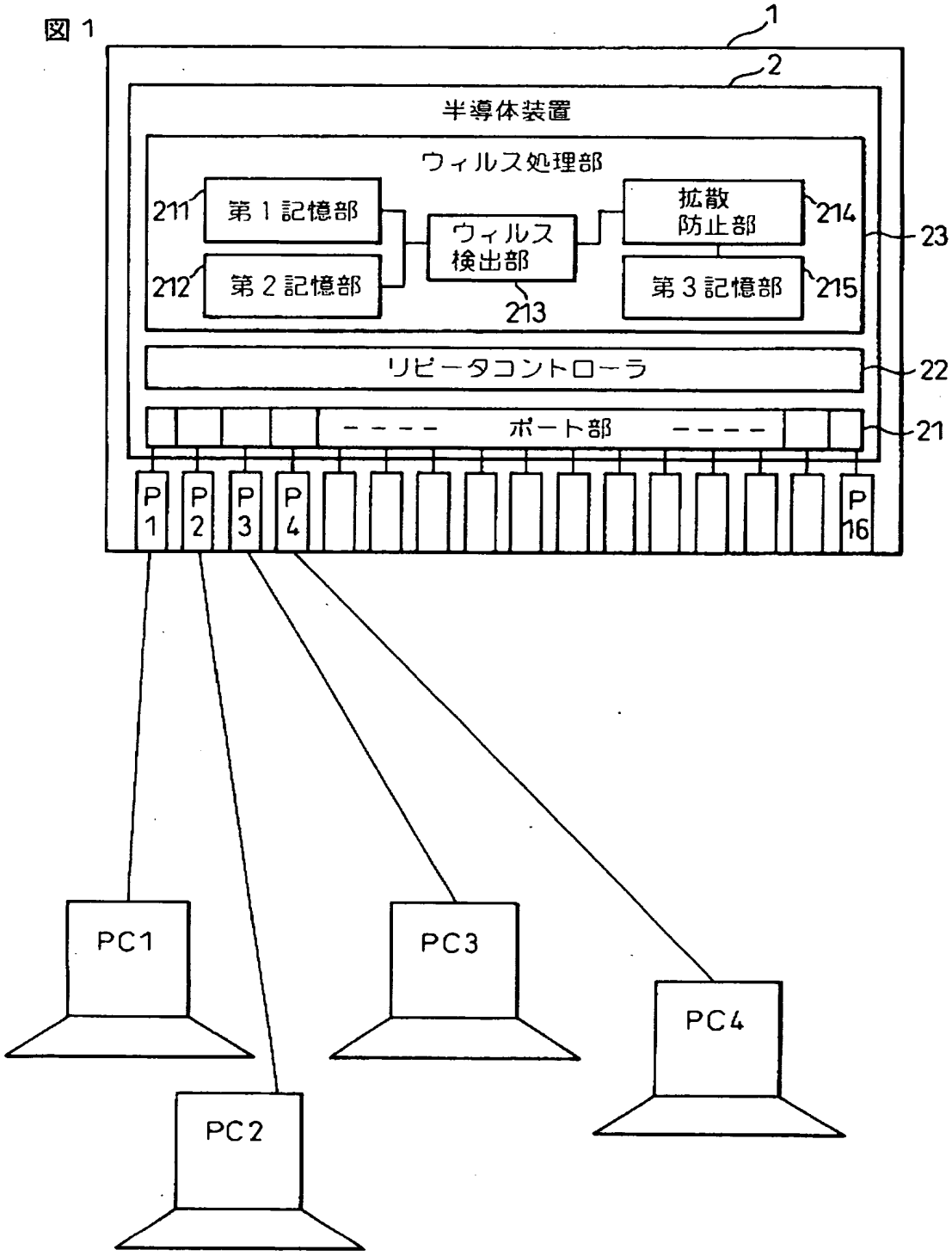
１２２ｂ、２１４…拡散防止部

２１３…ウィルス検出部

【書類名】　　図面

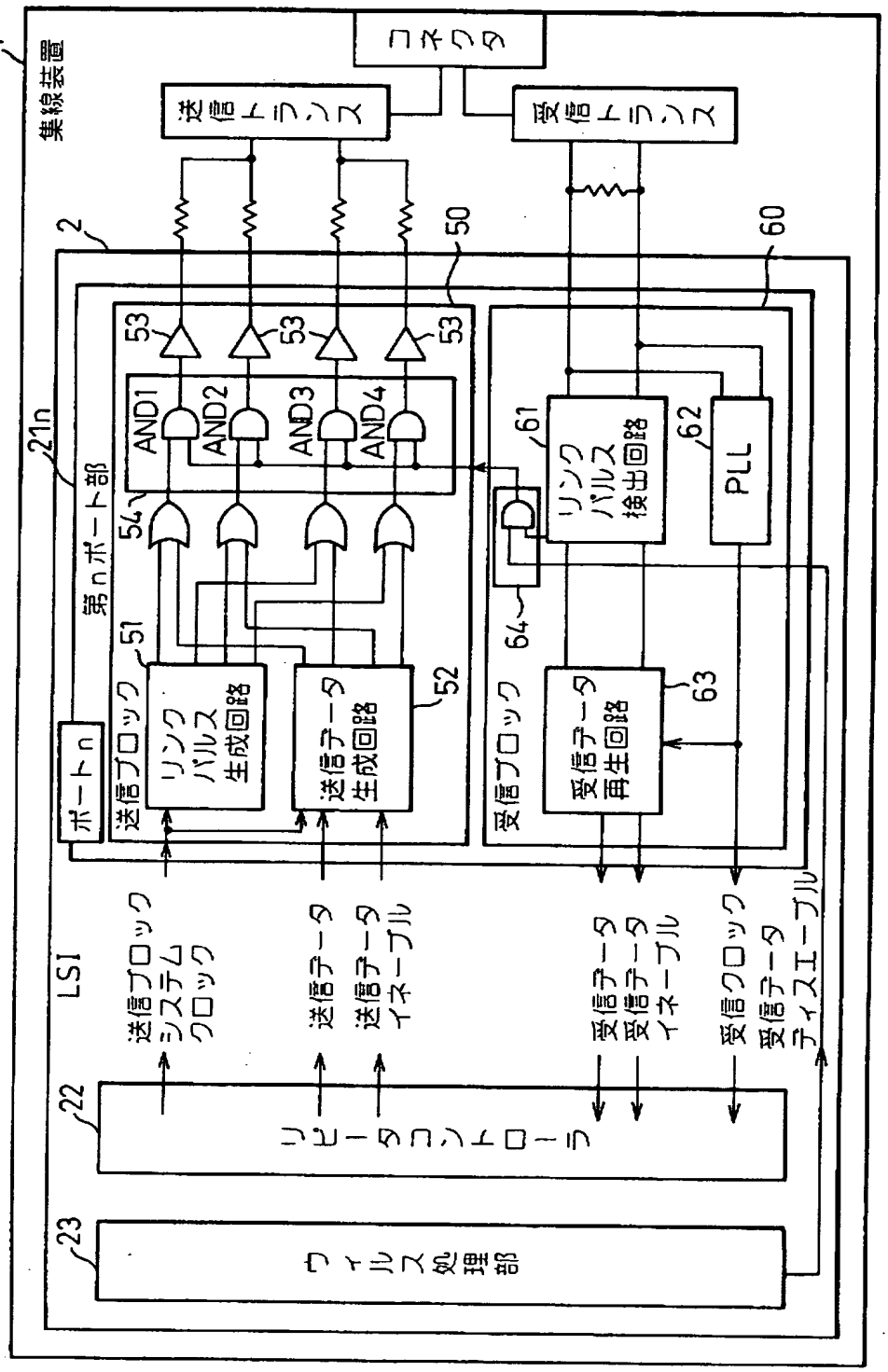
【図１】

図１


1
2
半導体装置
ウィルス処理部
211
第１記憶部
212
第２記憶部
ウィルス
検出部
213
拡散
防止部
214
第３記憶部
215
23
リピータコントローラ
22
ポート部
21
P
1
P
2
P
3
P
4
P
16
PC1
PC2
PC3
PC4

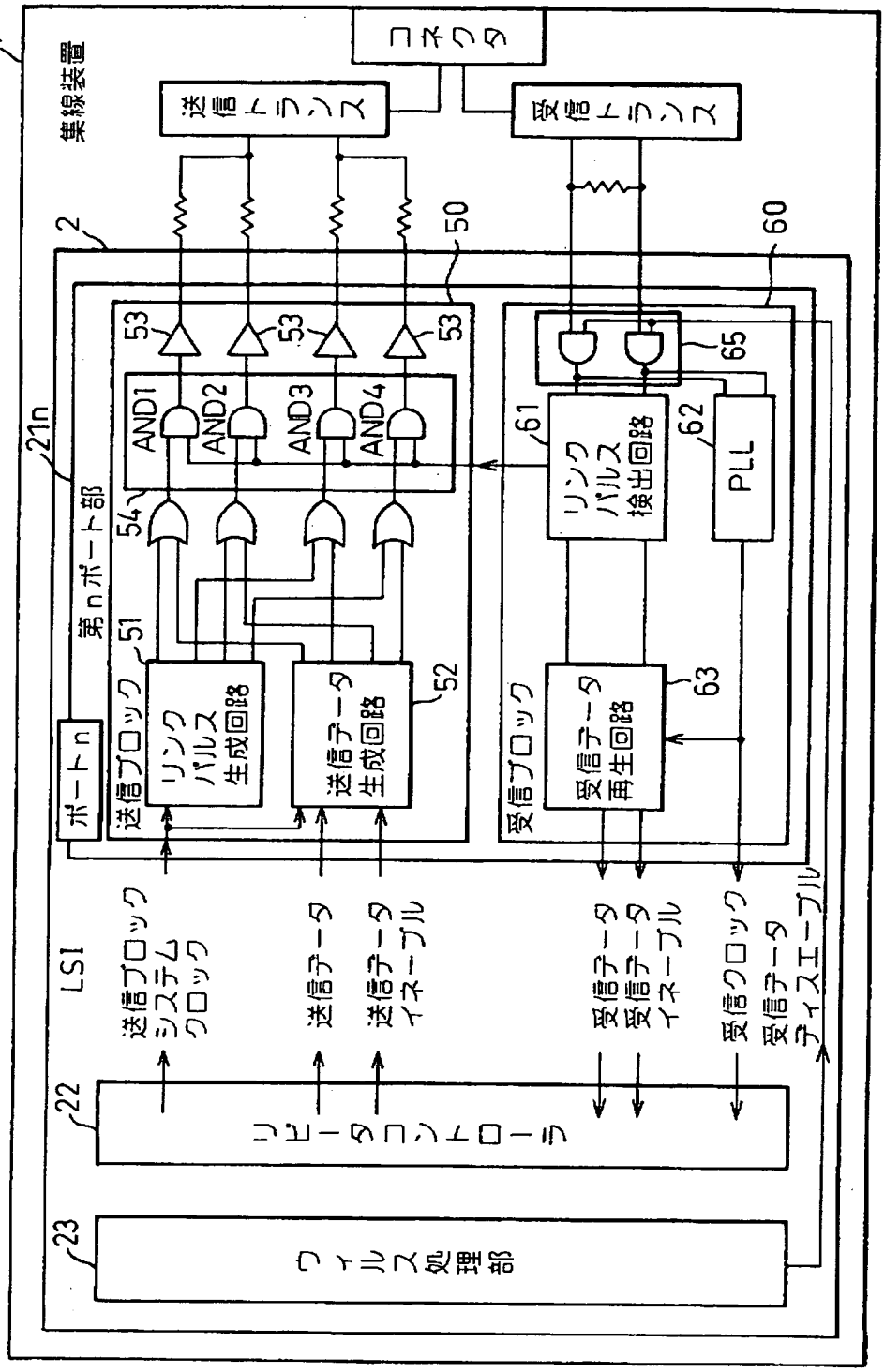
【図２】

図２


集線装置
1
コネクタ
受信トランス
受信トランス
2
50
60
53
53
53
AND1
AND2
AND3
AND4
21n
第nポート部
54
61
リンク
パルス
検出回路
62
PLL
64
51
送信ブロック
リンク
パルス
生成回路
送信データ
生成回路
52
受信ブロック
受信データ
再生回路
63
ポートn
LSI
送信ブロック
システム
クロック
送信データ
送信データ
イネーブル
受信データ
受信データ
イネーブル
受信クロック
受信データ
ディスエーブル
22
リピータコントローラ
23
ウィルス処理部

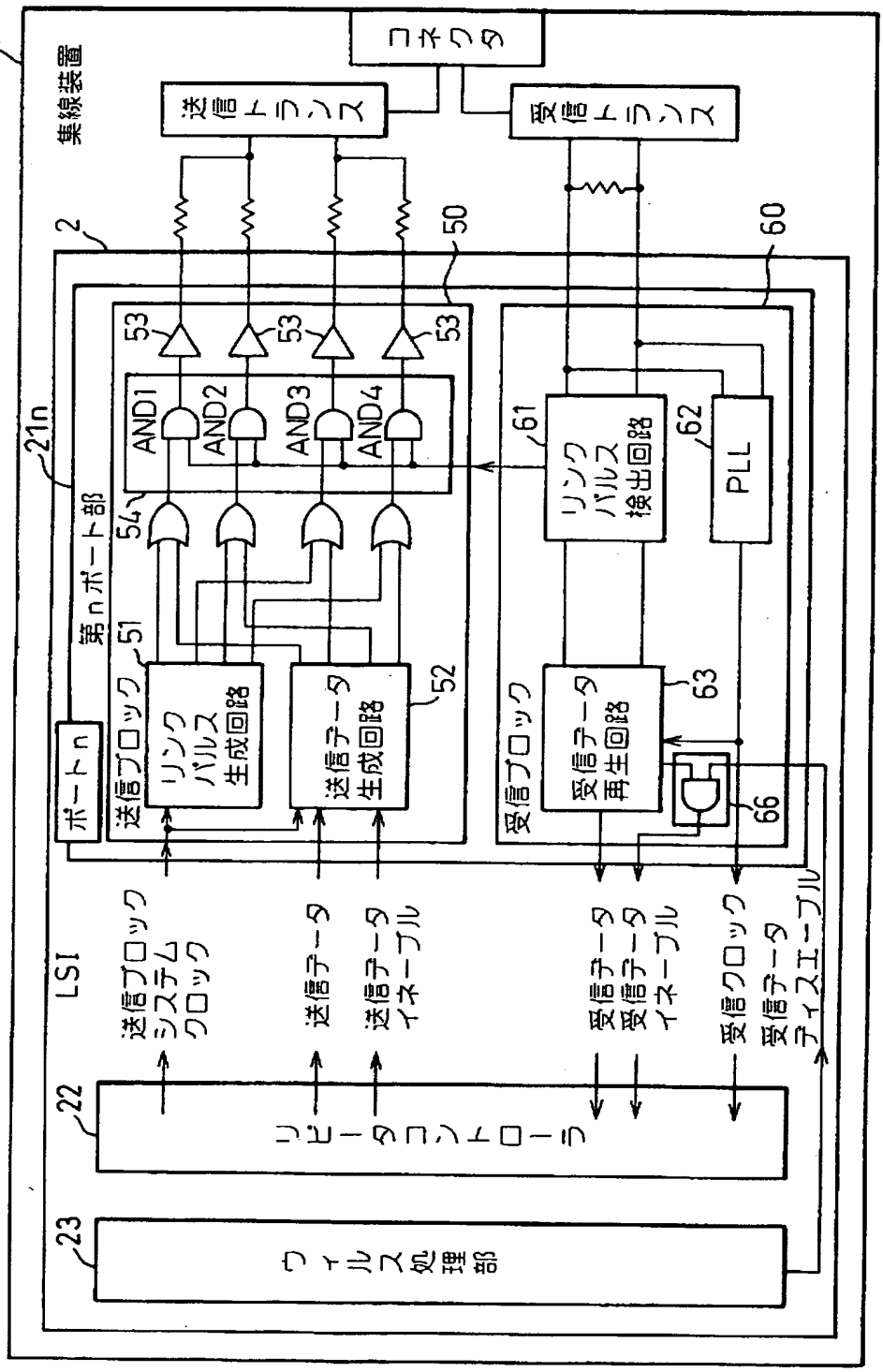
【図３】

図３


集線装置
コネクタ
送信トランス
受信トランス
2
50
60
53
53
53
65
AND1
AND2
AND3
AND4
21n
61
62
リンク
パルス
検出回路
PLL
54
第ｎポート部
51
52
63
ポートｎ
送信ブロック
リンク
パルス
生成回路
送信データ
生成回路
受信ブロック
受信データ
再生回路
LSI
送信ブロック
システム
クロック
送信データ
送信データ
イネーブル
受信データ
受信データ
イネーブル
受信クロック
受信データ
ディスエーブル
22
コントローラ
23
ウィルス処理部

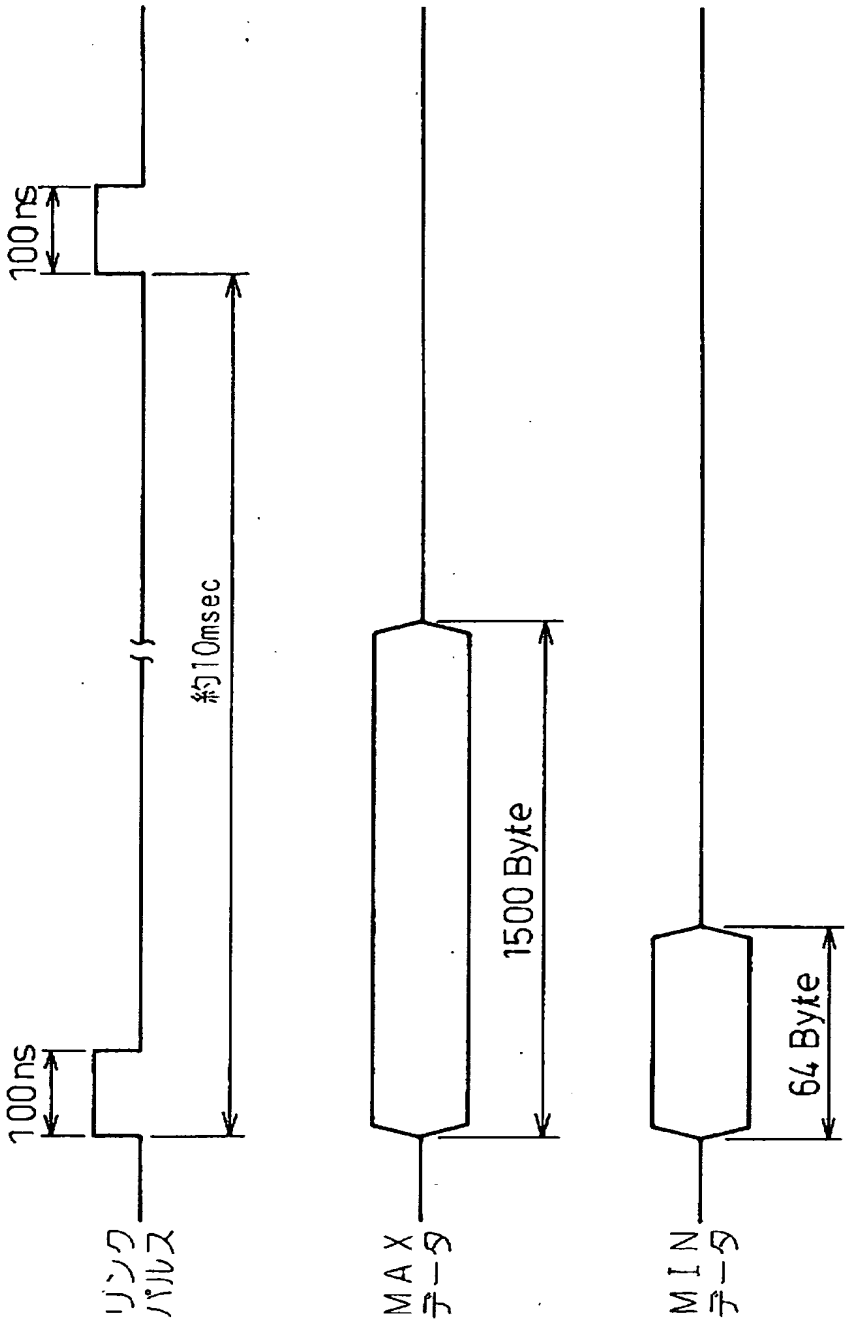
【図４】

図４


集線装置
コネクタ
送信トランス
受信トランス
2
50
60
53
AND1
AND2
AND3
AND4
54
21n
第nポート部
ポートn
送信ブロック
51
リンクパルス生成回路
送信データ生成回路
52
61
リンクパルス検出回路
62
PLL
受信ブロック
受信データ再生回路
63
66
LSI
送信ブロックシステムクロック
送信データ
送信データイネーブル
受信データ
受信データイネーブル
受信クロック
受信データディスエーブル
22
リピータコントローラ
23
ウィルス処理部

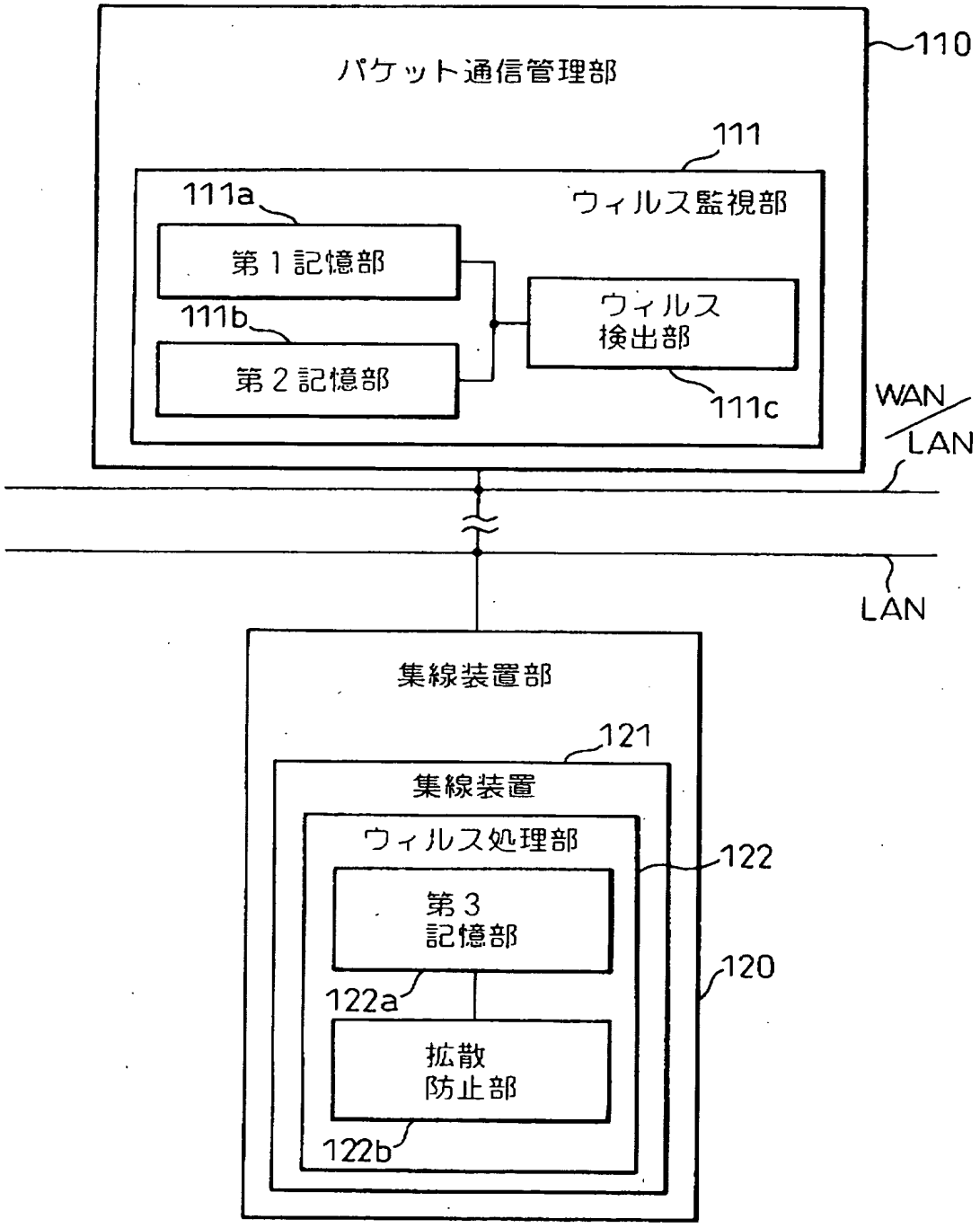
【図５】

図５



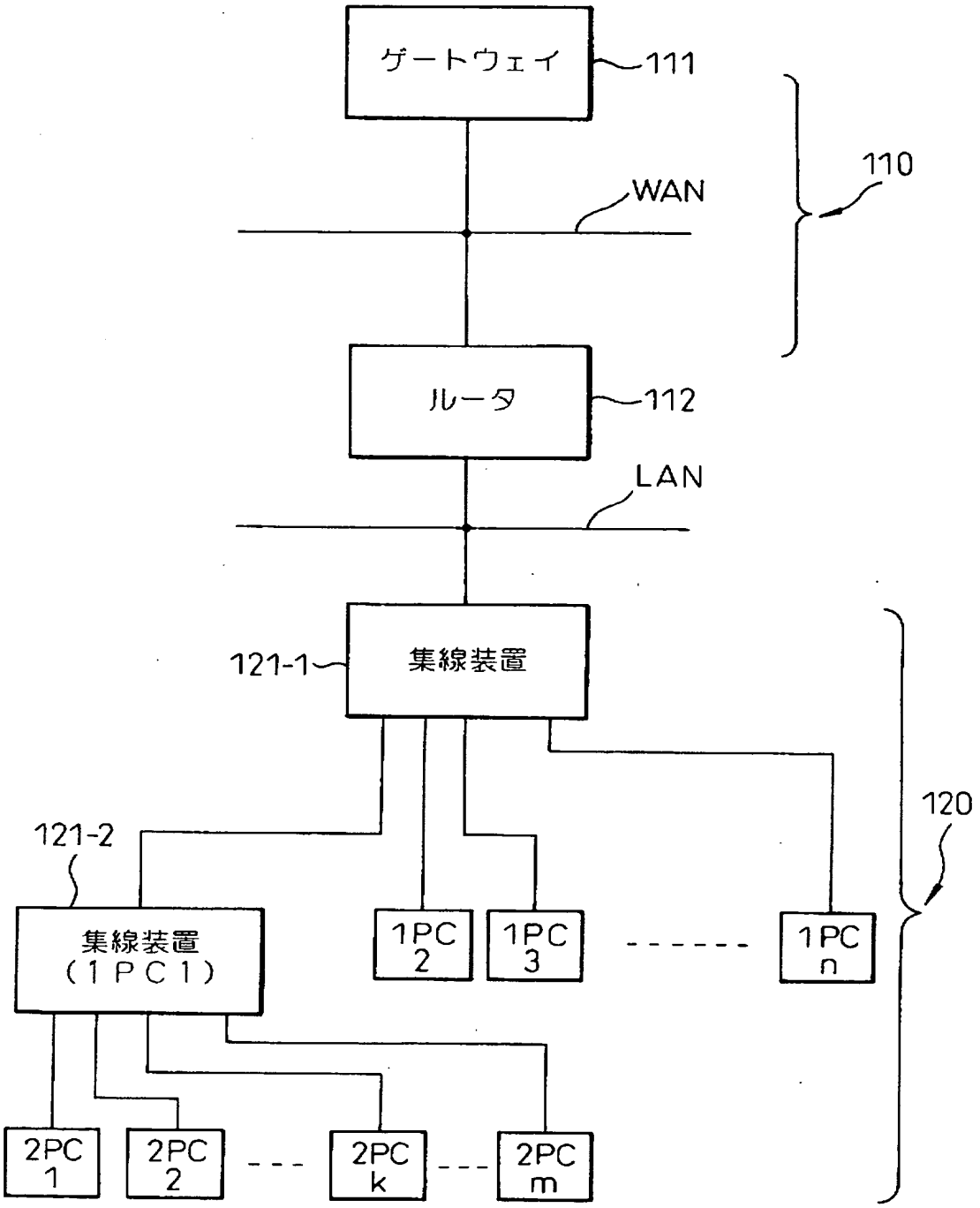
【図６】

図６


パケット通信管理部
110
111
ウィルス監視部
111a
第１記憶部
111b
第２記憶部
ウィルス
検出部
111c
WAN
LAN
LAN
集線装置部
121
集線装置
ウィルス処理部
122
第３
記憶部
120
122a
拡散
防止部
122b

【図７】

図７


ゲートウェイ
111
110
WAN
ルータ
112
LAN
121-1
集線装置
120
121-2
集線装置
（１ＰＣ１）
1PC
2
1PC
3
1PC
n
2PC
1
2PC
2
2PC
k
2PC
m

【書類名】　　要約書

【要約】

【課題】　通信装置にウィルス侵入防止対策せずウィルス侵入を防止する。

【解決手段】　ウィルスの検出情報を格納する第１記憶部２１１、受信データを一時蓄積する第２記憶部２１２、記憶部２１１に格納されたウィルスの検出情報と記憶部２１２に一時蓄積されたデータとを比較しデータがウィルスに感染しているか判定するウィルス検出部２１３、ウィルス検出部２１３でデータがウィルスに感染していると判定されたとき、受信データを集線装置１の外部に送信させない拡散防止部２１４および集線装置１に接続された通信装置のＭＡＣアドレスを格納する第３記憶部２１５を備える。拡散防止部２１４は、データのウィルス感染と判定されたデータに付されたデータ送信先通信装置のアドレスが記憶部２１５に格納されているＭＡＣアドレスに一致したときそのアドレスに対応する通信装置にデータを送信させない。

【選択図】　　図１

特願２００２－３３５４０９

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　神奈川県川崎市中原区上小田中１０１５番地
氏　名　　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社